I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Managing Digital Rights Management: Effectively Protecting Intellectual Property and Consumer Rights in the Wake of the Sony CD Copy Protection Scandal

JEREMY STANLEY*

Abstract: In 2005, Sony shipped millions of compact discs ("CDs") containing Digital Rights Management ("DRM") software. The software acted much like spyware, in that it allegedly installed itself on user computers without consent, concealed its presence on user computers, monitored user activity, and collected and transmitted data regarding user listening habits. The result was a public uproar, with many users calling for a boycott of Sony products due in part to the software creating serious privacy concerns. In response, Sony defended its product by claiming that the software included on its CDs was merely a DRM measure designed to protect its intellectual property rights.

In the aftermath of this controversy, it remains unsettled whether, in the future, other entertainment companies will attempt to enforce their intellectual property rights through DRM measures. Such future attempts to implement DRM may lead to other consumer protection violations not covered by currently existing legal remedies. This possibility, combined with the fact that DRM may already take away consumer rights under preexisting copyright law, suggests the need for an entirely different statutory scheme that regulates exactly what types of DRM measures copyright owners may take.

This comment explores these concerns by: (1) providing background information about DRM; (2) discussing the facts

* J.D. candidate, May 2008, Texas Tech University School of Law, Lubbock, Texas; B.S. in Computer Science and B.M. in Music Performance, May 2005, Texas Tech University, Lubbock, Texas.

surrounding the Sony scandal, describing the technology that Sony used, and providing details regarding the legal consequences that Sony faced as a result of its actions; and (3) proposing possible solutions to overreaching DRM schemes. Although current legal remedies may properly deter copyright owners from mimicking Sony's actions in the future, the Sony CD copy protection scandal illuminates the need for consumer protections requiring explicit disclosure, stringent standards for what DRM software can and cannot do, and independent review of DRM to ensure compliance.

I. INTRODUCTION: WHAT YOU DON'T KNOW CAN HURT YOU

Imagine, for a moment, that you have just arrived at your office. You log on to your computer, check your e-mail, and launch your web browser to perform some legal research. Wishing to enhance your work experience, you decide to insert a music compact disc ("CD"), given to you last weekend as a birthday present, into the CD drive of your computer. Much to your surprise, the media player program that you usually utilize to listen to CDs on this computer does not automatically begin playing your CD; instead, an end-user license agreement ("EULA") appears on your computer monitor. Being the seasoned professional that you are, you skim through the EULA and conclude that the music CD contains standard digital rights management ("DRM") software and that agreeing to it will allow you to listen to your CD, albeit only on the proprietary media player provided with the CD. Seeing no problem with this, you agree, and continue with your research. When the CD reaches the end of its final track, you eject the CD and continue with your work, believing that nothing is amiss. Unfortunately for you, your new CD—completely without your knowledge—has just installed software that will continue to run on your computer after you have ejected the CD. This software will hide its constituent files and associated information, drain your computer's resources, and create security holes that may subject your computer to viruses and compromise confidential personal and client information.

The situation described above may sound overly dramatic, but is realistic in light of the Sony BMG CD copy protection scandal.[1] Mark Russinovich, the man who discovered Sony's secretly installed software, known as a "rootkit,"[2] posted his findings on his blog on October 31, 2005.[3] Sony had already shipped 4.7 million CDs

---

[1] *See, e.g.*, John Borland, *Sony CD Protection Sparks Security Concerns*, CNET NEWS.COM, Nov. 1, 2005, http://news.com.com/Sony+CD+protection+sparks+security+concerns/2100-7355_3-5926657.html.

[2] A rootkit is "[a] type of Trojan that keeps itself, other files, registry keys and network connections hidden from detection." *See* Definition of: rootkit, PC MAGAZINE, http://www.pcmag.com/encyclopedia_term/0,2542,t%3Drootkit&i%3D55733,00.asp (last visited Mar. 11, 2008).

[3] Mark's Blog, http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx (Oct. 31, 2005, 11:04 CST).

containing the software over a period of eight months, and by the time the software was discovered, over 2.1 million of those CDs had been sold.[4] Serious concerns over computer security led to public uproar and a subsequent call to boycott Sony products.[5] In response, Sony claimed that the software included on its CDs was merely a DRM measure designed to protect its intellectual property rights.[6]

Less than a month later, Texas Attorney General Greg Abbott sued Sony under the Texas Consumer Protection Against Computer Spyware Act, alleging that "SONY ha[d] engaged in a technological version of cloak and dagger deceit against consumers by hiding secret files on their computers . . . . Consumers who purchased a SONY CD thought they were buying music. Instead, they received spyware that can damage a computer, subject it to viruses and expose the consumer to possible identity crime."[7] The Texas Spyware Act took effect on September 1, 2005, just two months prior to the discovery of Sony's rootkit and, coincidentally, the Texas suit was the first spyware enforcement action in the United States.[8] The lawsuit sought $100,000 for each violation, the maximum penalty under the Texas Spyware Act.[9]

Following the Texas filing, Sony became the subject of investigations by thirty-nine states, the District of Columbia, the

---

[4] John Borland, *Sony Recalls Risky 'Rootkit' CDs*, CNET NEWS.COM, Nov. 15, 2005, http://news.com.com/Sony+recalls+risky+rootkit+CDs/2100-7349_3-5954154.html.

[5] Brian Krebs, *Study of Sony Anti-Piracy Software Triggers Uproar*, WASH. POST, Nov. 2, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/11/02/AR2005110202362.html.

[6] *Id.* The protection measure utilized by Sony on its CDs is more appropriately referred to as copy protection (which is any technological measure designed to prevent copying), but the author will refer to copy protection and DRM (which is far broader than copy protection because content owners can regulate more than just copying under DRM schemes) synonymously throughout this comment because it is the author's intention that many of the concepts, legal principles, and solutions apply equally to copy protection and DRM.

[7] Press Release, Texas Attorney General Greg Abbott, Attorney General Abbott Brings First Enforcement Action in Nation Against Sony BMG for Spyware Violations (Nov. 21, 2005), *available at* http://www.oag.state.tx.us/oagnews/release.php?id=1266 [hereinafter Abbott Press Release].

[8] *Id.*

[9] *Id.*

Federal Trade Commission, and foreign governments.[10] The basis of these investigations was an allegation that Sony's CDs contained software that created security holes[11] and was difficult to remove, and that Sony had failed to inform consumers of the nature of the software. For example, former Ohio Attorney General Jim Petro stated that Sony's DRM software may have violated Ohio's Consumer Sales Practices Act, which requires that all terms of a product be disclosed to consumers before they buy the product.[12] Moreover, consumers filed several individual and class action lawsuits against Sony.[13] These lawsuits sought damages based on a variety of statutory and common law theories: unlawful, unfair, and fraudulent business practices; misrepresentation; trespass; breach of implied covenant of good faith and fair dealing; and breach of warranty.[14] Sony negotiated to settle these lawsuits and to quell investigations by agreeing to pay various amounts to the individual states and consumers harmed by Sony's DRM software. In accordance with the settlement terms, Sony agreed to take action to reverse the effects of its DRM software, and to limit its future use of DRM software.[15]

While legal principles such as trespass, conversion, breach of warranty, and fraud, as well as existing laws such as anti-spyware legislation and consumer protection statutes, may provide an effective penalty for behavior such as Sony's, application of such legal principles and law may prove to be problematic.[16] For example, one commentator has noted that most state anti-spyware legislation is probably unconstitutional, tends to be overly regulatory, and will most

---

[10] *See* discussion *infra* Part III.D.

[11] One security issue that Sony's software created was that unauthorized users could take advantage of the software's rootkit-like cloaking functionality (by simply adding "sys" to the beginning of a file name) to hide any file (including viruses and other malicious software) regardless of whether that file was associated with Sony's software or came from a completely unrelated source. J. Alex Halderman, *CD DRM Makes Computers Less Secure*, FREEDOM TO TINKER, Nov. 1, 2005, http://www.freedom-to-tinker.com/?p=919.

[12] *See* discussion *infra* Part III.D.

[13] *See* discussion *infra* Part III.E.

[14] *See* discussion *infra* Part III.E.

[15] *See* discussion *infra* Part III.D–E.

[16] Susan P. Crawford, *First Do No Harm: The Problem of Spyware*, 20 BERKELEY TECH. L.J. 1433, 1436 (2005).

likely be unsuccessful in stemming the flow of spyware.[17] Furthermore, pending federal anti-spyware legislation will preempt state bills if enacted,[18] and even if anti-spyware legislation survives the preceding criticisms, it does not seem appropriately suited to address the full scope of the situation illustrated by the Sony scandal.

There are additional factors that mitigate the effectiveness of existing legal remedies when dealing with invasive and harmful DRM measures. Under the current legislative scheme, there is a real possibility that many consumers will unknowingly be harmed by hidden DRM software. Such prospective harms are enhanced by the average consumer's relative inability to recognize and analyze the effects of intrusive and stealthy DRM software on technological systems. Additionally, even if consumers know they have suffered harm, some may believe they have no recourse or that it is simply not worthwhile to pursue legal action against the offending content provider.

However, the need to protect consumer interests in privacy and security must be balanced against copyright owners' interest in fully protecting their intellectual property. While the Digital Millennium Copyright Act ("DMCA") protects copyright owners' use of DRM and other technological protection measures, it provides no guidance regarding what types of technological protection are legitimate, as opposed to those that are abusive. Allowing widely varying state statutory and common law to provide this missing definition places a great burden on copyright owners who wish to design their respective DRM measures to avoid liability; allowing this variance may also run afoul of the general preemption of state laws affecting matters within the DMCA. A uniform set of legal principles governing the use of DRM measures may be more desirable than leaving such regulation to the existing hodgepodge of state law. Moreover, if such uniform legislation were to be established, preemptive regulation of DRM measures—as opposed to retrospective relief—may go a long way toward alleviating the possibility that consumers will be unable to protect themselves from, or even detect, abusive DRM measures.

If the software that Sony placed on its CDs was intended solely as a DRM measure, it stands to reason that Sony and other entertainment companies will continue to try to enforce their

---

[17] *See, e.g., id.*

[18] Josh Sugnet, Comment, *Catching a Black Cat in a Dark Room: Evaluating the Shortcomings of Federal and State Anti-Spyware Legislation*, 28 HASTINGS COMM. & ENT. L.J. 443, 458 (2006).

intellectual property rights through similar measures in the future.[19] Assuming that this is so, such future attempts to implement DRM may lead to other consumer protection violations not covered by anti-spyware legislation or other consumer protection statutes. This possibility, combined with the fact that DRM may already take away consumer rights established under preexisting copyright law, suggests the need for an entirely different body of law that regulates exactly what types of DRM measures Sony and similarly situated companies may take.[20]

This comment explores these concerns. Part II provides background information on DRM. Part III discusses the facts surrounding the Sony scandal, describes the technology that Sony used, and provides details regarding the Texas and other lawsuits filed against Sony. Finally, Part IV proposes possible solutions to overreaching DRM schemes. Although anti-spyware legislation may properly deter Sony and similar companies, the Sony CD copy protection scandal illuminates the need for consumer protection against DRM measures in the form of regulations requiring explicit disclosure, stringent standards for what DRM software can and cannot do, and independent review of DRM to ensure compliance.

II. DIGITAL RIGHTS MANAGEMENT

A. BACKGROUND

DRM technology attained widespread use following the advent of the digital age.[21] The prevalence of many different types of copyrightable works in digital form, such as music, movies, literary works, and software, along with the availability of easy-to-use and inexpensive technology enabling replication, distribution, and high-speed Internet access, has resulted in many more potential infringers of copyrighted material.[22] This increase in the number of infringers and cases of infringement has also increased the cost of monitoring and enforcing against intellectual property rights violations under

---

[19] *See* Krebs, *supra* note 5.

[20] *See* Michael Geist, *Legal Fallout from Sony's CD Woes*, BBC NEWS, Jan. 3, 2006, http://news.bbc.co.uk/2/hi/technology/4577536.stm.

[21] Dan L. Burk, *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537, 538 (2005).

[22] *See id.*

existing law.[23] To protect their intellectual property rights in this new climate, many digital content companies now employ technology-based restrictions on use of company-owned content.[24] In doing so, these companies essentially forego established legal remedies and resort to what amounts to "self-help": technological standards created by the content provider to replace or enhance established legal protections.[25]

In describing DRM technologies, Dan L. Burk notes:

> [D]igital technologies carry the capacity to embody highly sophisticated behavioral inscriptions that can accompany copies of a creative work as they are distributed, controlling uses of the work. Consequently, because digital technologies can be scripted to accommodate a variety of user behaviors, such controls can be scripted to incorporate restrictions that might otherwise be the subject matter of a written license.[26]

In other words, DRM technologies, much like licenses, can limit consumers' use of intellectual property. A key distinction between DRM and contractual licenses, therefore, is enforcement. Licenses rely heavily on licensees actually conforming their behavior as agreed under contract, while DRM technologies place real, technological limitations on what users may do with the intellectual property.[27] Moreover, licenses pose added enforcement obstacles since the governing terms may be held unconscionable; may constitute a contract of adhesion, or may be unenforceable under state law.[28] The absence of potential contractual liability allows DRM technologies to provide immediate and uniform enforceability with a reduced incidence of litigation, at least until the present scandal. Use of DRM

---

[23] *Id.*

[24] Declan McCullagh & Milana Homsi, *Leave DRM Alone: A Survey of Legislative Proposals Relating to Digital Rights Management Technology and Their Problems*, 2005 MICH. ST. L. REV. 317, 318 (2005).

[25] Burk, *supra* note 21, at 538.

[26] *Id.* at 546 (citation omitted).

[27] *See id.*

[28] *See* Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 269 (5th Cir. 1988) (noting that the district court held the license to be an adhesion contract that would only be enforceable if allowed by state law).

technologies is attractive to intellectual property owners for several reasons: (1) restrictions on the use of intellectual property are limited only by owner discretion and not by what Congress and the courts have provided under the Copyright Act of 1976; (2) the owner does not have to worry about contractual or license provisions surviving the scrutiny of the courts because DRM technologies turn restrictions previously found in licenses and contracts into inherent properties of content-based products; and (3) DRM technologies lessen the expense of enforcing restrictions by limiting user behavior instead of relying on users to conform their behavior.[29]

A specific example of DRM technology is the Windows Media DRM, which is designed for use with digital audio and video files and live broadcasting over the Internet.[30] According to Microsoft, this technology is available for personal computers, portable devices, and network devices.[31] The software locks digital files with a unique "license key," and encrypts the files so that it is considerably more difficult to create pirated copies.[32] The assignment of a unique license key makes it possible to associate each instance of the Windows Media Player software with one computer; every time a user wants to play a file, the DRM technology ensures that the user has permission to play that file by checking the user's license key.[33] The technology also protects the audio stream as it travels from the media player software to the computer's sound card (to prevent programs from copying content from the audio stream), and provides ways for content owners to specify different rights for different types of devices. Finally, Windows Media DRM may "control license start times, stop times, and duration" and create purchase, rental, and subscription plans for consumers.[34]

---

[29] *Id.* at 544–48. For more information of digital rights management, *see* Ariel Katz, *The Potential Demise of Another Natural Monopoly: New Technologies and the Administration of Performing Rights*, 2 J. COMPETITION L. & ECON. 245, 248–52 (2006).

[30] Microsoft.com, Features of Windows Media DRM, http://www.microsoft.com/windows/windowsmedia/forpros/drm/features.aspx (last visited Mar. 11, 2008).

[31] *Id.* (describing features for "devices such as portable audio and video players, set-top boxes, and mobile devices with audio and video capabilities" and "DVD players, digital media receivers, and digital audio receivers").

[32] *Id.*

[33] *Id.*

[34] *Id.*

Other corporations have successfully utilized DRM technology to protect the distribution of their product. To address internal concerns that its Norton Antivirus 2003 software is one of the most widely pirated computer applications on the market, Symantec started distributing copies of the program that are protected by DRM software.[35] While Symantec will not reveal what software it is using, or the identity of the software's creator, it is known that users will have to download an activation key and activate the software within fourteen days of installation. Once the activation key has been authenticated by Symantec's servers, users may run the antivirus software, but the DRM software will limit their behavior to comply with the software's EULA.[36]

Other examples of recent uses of DRM technologies are Adobe's Acrobat 7 and LiveCycle.[37] These programs provide a wide array of options for content creators that wish to control access to, and use of, their intellectual property.[38] Some of these options include placing limitations on printing and modification of documents, as well as tracking use and setting expiration dates.[39] Finally, courts have heard claims regarding DRM and copy protection measures for protecting intellectual property as diverse as garage door opener software,[40] music CDs,[41] motion picture DVDs,[42] computer games,[43] and

---

[35] Mark Hachman, *Symantec Adds DRM to Norton Antivirus*, EXTREMETECH, Apr. 8, 2003, http://www.extremetech.com/article2/0,1697,1164289,00.asp.

[36] *Id.*

[37] John Bringardner, *The Three Types of PDF Security*, PDFZONE, Sept. 7, 2005, http://www.pdfzone.com/c/a/Document-Management/The-Three-Types-of-PDF-Security/.

[38] *Id.*

[39] *Id.*

[40] Chamberlain Group, Inc. v. Skylink Techs., Inc., 292 F. Supp. 2d 1023, 1040 (N.D. Ill. 2003) (finding that the plaintiff had not established a connection between the defendant's universal remote control and unauthorized use of the plaintiff's copyrighted garage door opener software).

[41] *See, e.g.*, Keel v. BMG Entertainment, No. B164476, 2003 WL 22808378, at *1 (Cal. Ct. App. Nov. 26, 2003) (describing controversy relating to the defendant's failure to provide notice that DRM technology on its music CDs impaired performance).

[42] *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435 (2d Cir. 2001) (affirming a permanent injunction against making available computer software for Decoding Content Scrambling System-encrypted motion picture DVDs); Paramount

"system[s] for distributing, retrieving and playing digital audio and video content via the Internet."[44]

The current technological and legal landscape presents a temptation for copyright owners to misuse DRM. First, DRM exists in a wide variety of forms; it may either accompany individual content-based products in hard-copy (e.g., CD, Blu-Ray Disc, or DVD) or digital file (e.g., content files or software distributed over the Internet) forms, or it may be integrated with devices providing access to content based products, such as personal computer operating systems.[45] Moreover, DRM technology accompanying individual content-based products may perform a dual role of controlling access to the individual product that it accompanies and integrating with devices to control access to other content-based products.[46] Second, the DMCA lacks guidelines pertaining to what types of DRM and other technological protection measures are permissible, and grants copyright owners vast freedom to determine how their respective DRM technologies should be implemented. Third, consumers have no expectation that products in the marketplace will have concealed features that operate contrary to their security interests. Finally, because copyright law grants a monopoly to copyright holders, consumers may have no access to equivalent alternatives lacking DRM software. This current combination of technological flexibility, lack of

---

Pictures Corp. v. 321 Studios, No. 03-CV-8970 (RO), 2004 WL 402756 (S.D.N.Y. Mar. 3, 2004) (granting preliminary injunction against identical software); Macrovision v. Sima Prods. Corp., No. 05-CV-5587 (RO), 2006 WL 1472152, at *1–2 (S.D.N.Y. May 26, 2006) (denying a motion to reconsider preliminary injunction that the court issued against defendant's DVD copy protection circumvention products and stating that "hinder[ing] the making of videotape copies of protected DVDs . . . is among a copyright owner's rights").

[43] Sony Computer Entm't Am., Inc. v. Divineo, Inc., 457 F. Supp. 2d 957, 959 (N.D. Cal. 2006) (granting the plaintiff's motion for summary judgment of a DMCA claim against the defendant for producing devices that circumvent the Sony Playstation video game console's authentication process).

[44] RealNetworks, Inc. v. Streambox, Inc., No. 2:99CV02070, 2000 WL 127311, at *1–2 (W.D. Wash. Jan. 18, 2000) (enjoining the defendant from generally making available certain products that allow users to circumvent or modify technological security measures that plaintiff designed to protect copyright owner's intellectual property available over the Internet in streaming and downloadable formats).

[45] *See* discussion *supra* notes 31–45 and accompanying text.

[46] The ability to interface with a device providing access to content may also grant the ability to alter the operation of that device or to access personal user information stored on the device.

clear legislative guidance, consumer ignorance, and absence of alternative products has created a potentially powerful temptation for copyright owners to misuse DRM technology.

B. CONFLICTS WITH CONSUMER RIGHTS

1. THE COPYRIGHT ACT OF 1976

At its core, the Copyright Act of 1976 represents a bargain between the public and authors.[47] In return for a grant of certain exclusive rights to authors and other copyright owners, the public receives certain other rights with respect to copyrighted work, as well as the benefit of access to new expression and knowledge, which ostensibly contributes to the advancement of society as a whole.[48] Because the DMCA provides penalties for circumvention of technological protection measures, it essentially provides an incentive for copyright owners to use DRM and related technologies, leading critics of the DMCA to claim that the DMCA has allowed the privatization of copyright law.[49]

Critics of DRM technology point out that the copyright owners who limit use of their works with DRM technology can impose conditions that restrict rights consumers would normally possess under the Copyright Act of 1976.[50] For example, the Copyright Act of 1976 allows for consumers of copyrighted material to assert fair use as a defense against copyright owners' claims of infringement.[51] Other

---

[47] 17 U.S.C. §§ 101–810, 1101 (1976).

[48] Stacy F. McDonald, Comment, *Copyright for Sale: How the Commodification of Intellectual Property Distorts the Social Bargain Implicit in the Copyright Clause*, 50 HOW. L.J. 541, 544–51 (2007).

[49] *Id.* at 564.

[50] Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1998 (2006). Copyright owners can impose any restriction on consumer use they wish, limited only by what it technologically possible at any given time. *Id.*

[51] Copyright Act of 1976, 17 U.S.C. § 107 (2000). Fair use can include use "for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research." *Id.* Other uses of copyrighted material may also constitute fair use; courts consider four factors, including the "purpose and character of the use," "nature of the copyrighted work," "amount and substantiality of the portion used," and the "effect of the use upon the potential market for or the value of the copyrighted work." *Id.*

defenses under the Copyright Act of 1976 allow users of copyrighted works to claim justifiable reproduction by libraries and archives[52] and transfer or sale.[53]

Potentially, DRM technology restricts such lawful uses, which were unambiguously codified under the Copyright Act of 1976.[54] Furthermore, in the absence of an encoded expiration date, DRM schemes are inextricably embedded in the work that they protect and will continue to prevent users from lawful use, long after the copyright term has expired and the work has entered the public domain.[55]

2. OTHER CONSUMER RIGHTS

In addition to providing copyright owners with the ability to deny rights provided to consumers under the Copyright Act of 1976, use of DRM creates the potential for violations of other consumer rights. As noted above, several factors create the temptation for copyright holders to misuse DRM, including: (1) the lack of restriction on how DRM technologies may operate; (2) the ability to design DRM to interface with, alter the operation of, and access information stored on devices providing access to copyrighted works; (3) the public's expectation that products in the marketplace are generally safe to use; and (4) the unavailability of alternative identical products to consumers with respect to copyrighted works. The pervasive potential for misuse has led commentators to complain that if left unregulated, DRM may result in consumers being subjected to surveillance by copyright owners.[56] Moreover, poorly designed DRM technologies can create security problems, drain resources, or simply render the associated copyrighted work incompatible with devices that are

---

[52] *Id.* § 108.

[53] *Id.* § 109. This would likely be limited in a DRM context to uses such as electronic lending or transfer, such as by a library. Zittrain, *supra* note 50, at 1998.

[54] Zittrain, *supra* note 50, at 1998.

[55] Daniel S. Hurwitz, Comment, *A Proposal in Hindsight: Restoring Copyright's Delicate Balance by Reworking 17 U.S.C. § 1201*, 13 UCLA ENT. L. REV. 263, 282–83 (2006).

[56] Chris Jay Hoofnagle, *Digital Rights Management: Many Technical Controls on Digital Content Distribution Can Create a Surveillance Society*, 5 COLUM. SCI. & TECH. L. REV. 1, 2 (2004), *available at* http://www.stlr.org/cite.cgi?volume=5&article=6; Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 580 (2003).

designed to provide access to copyrighted works.[57] To the extent that DRM technologies begin to take on a surveillance role, critics complain that "DRM technology is becoming increasingly indistinguishable from . . . spyware."[58]

The public began using the term "spyware" in 1999 to refer to many different types of unwelcome software, and as a result, several different definitions for the term exist.[59] Ari Schwartz, the Associate Director of the Center for Democracy and Technology, has broadly defined spyware as "unwanted software that sneaks onto computers without their owner's consent and cannot be uninstalled." Using increasingly derogatory language, New York Attorney General Elliot Spitzer referred to spyware as "fraudulent programs [that] foul machines, undermine productivity and in many cases frustrate consumers' efforts to remove them from their computers."[60]

Spyware can become integrated with a computer user's system in many different ways.[61] Sometimes, it is included in the installation of other software (and users may actually consent to the installation of the spyware by agreeing to a lengthy and complex EULA).[62] Spyware may also install itself onto a computer by exploiting Internet browsers and operating system security holes, or via virus, worm, or similar technology.[63] The Anti-Spyware Coalition ("Coalition") has neutrally defined spyware as follows:

---

[57] *See* Ian Thomson, *UK Consumer Group Calls for DRM Legislation*, VNUNET.COM, Jan. 17, 2007, http://www.pcw.co.uk/vnunet/news/2148685/consumer-group-calls; Dugie Standeford, *Governments Eye DRM Interoperability Rules as Consumers Vent Over Access*, INTELL. PROP. WATCH, Dec. 4, 2006, http://www.ip-watch.org/weblog/index.php?p=476&res=1280&print=0.

[58] Thomson, *supra* note 57.

[59] Sharon Weinbar, *The Spyware Inferno*, CNET NEWS.COM, Aug. 13, 2004, http://news.com.com/2010-1032-5307831.html.

[60] Press Release, Office of New York State Attorney General Andrew M. Cuomo, State Sues Major "Spyware" Distributor: Intermix Media Accused of Vast Pattern of Surreptitious Installations (Apr. 28, 2005), *available at* http://www.oag.state.ny.us/press/2005/apr/apr28a_05.html.

[61] *See* Sugnet, *supra* note 18, at 448–49.

[62] *Id.* at 448.

[63] *Id.*

> Technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:
>
> - Material changes that affect their user experience, privacy, or system security;
> - Use of their system resources, including what programs are installed on their computers; and/or
> - Collection, use, and distribution of their personal or other sensitive information. [64]

The Coalition also notes that many types of software that might be spyware can also perform functions that are helpful to computer users when installed on computers pursuant to proper notice, consent, and control. Therefore, whether users had appropriate notice, consent, and control over the software is an important factor in determining whether certain software actually constitutes spyware.[65]

Sony's rootkit-like DRM shared many attributes with the preceding definitions of spyware. As a result, Texas and California chose to apply their newly enacted spyware statutes to the DRM technology in litigation seeking redress for their respective citizens. While anti-spyware legislation may prove to be an effective method of dealing with overly intrusive DRM technology, it may also prove to be an invalid or inappropriate means for regulating DRM technology, especially in light of the fact that anti-spyware legislation was not specifically designed with DRM in mind. Copyright owners will possibly use spyware-like DRM technology in the future, and legislatures should be cognizant of the potential need for DRM-specific regulation.

A specific DRM technology tied to copyrighted software products often raises problems of "incompatibility." Either intentionally or through a design flaw, the supplementary devices can effectively limit access to the copyrighted work.[66] Incompatibility caused by DRM can

---

[64] Anti-Spyware Coalition, Anti-Spyware Coalition Definitions Document, http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm (last visited Mar. 11, 2008).

[65] *Id.* ("[A] keylogger can be used for legitimate purposes with clear consent, such as letting an [information technology] help desk remotely assist a user in problem diagnosis. An underlying technology typically becomes unwanted when it is implemented in a way that provides no benefit to—or actively harms—authorized users.").

[66] Standeford, *supra* note 57.

be harmful to consumers by limiting the devices available to access copyrighted material.[67] France has attempted to deal with this problem by revising its copyright law to require that copyright owners using DRM technology disclose information (such as software code) necessary to ensure interoperability.[68] Other European governments are currently considering legislation mandating interoperability as well, but similar legislation in the United States does not appear likely as of this writing.[69]

C. RATIFICATION BY THE DMCA

The DMCA's anti-circumvention provisions[70] indicate Congressional ratification of DRM technology use, and simultaneously create the potential for a serious consumer dilemma.[71] The DMCA prohibits three types of circumvention of protection technologies, including circumvention of access controls, "trafficking in technologies or devices that circumvent access controls, and . . . trafficking in technologies or devices that circumvent rights protection."[72] The DMCA exempts specific types of circumvention by some individuals and entities: (1) the Librarian of Congress; (2) nonprofit libraries, archives, and educational institutions; (3) law enforcement, government, and intelligence officers, agents, or employees; (4) purchasers of protected computer programs who need to reverse engineer those programs to ensure interoperability with other computer programs; (5) encryption researchers (typically those legitimately studying, employed in, or trained and experienced in, the encryption technology field); (6) parents wishing to limit the Internet access of their minor children; (7) persons wishing to prevent DRM technology from disseminating personal information; and (8) persons

---

[67] Center for Democracy and Technology, DRM Metrics–Effect on Use, http://www.cdt.org/copyright/20060907drm-metrics-effect-on-use.php (last visited Feb. 27, 2008).

[68] Standeford, *supra* note 57.

[69] *Id.*

[70] 17 U.S.C. §§ 1201–1205 (2000).

[71] *See* Hurwitz, *supra* note 55, at 276–80.

[72] Stephen E. Blythe, *The U.S. Digital Millennium Copyright Act and the E.U. Copyright Directive: Comparative Impact on Fair Use Rights*, 8 TUL. J. TECH. & INTELL. PROP. 111, 111 (2006). For the DMCA provision prohibiting these uses, *see* Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)–(b) (2000).

wishing to conduct testing for computer security purposes.[73] In addition, the DMCA allows the Librarian of Congress to make determinations as to the effect of the prohibition on circumvention of protection technologies on non-infringing uses and provide exemptions for classes of copyrightable works based on those determinations.[74]

Section 1201(c) of the DMCA indicates that the anti-circumvention provisions "shall [not] affect rights, remedies, limitations, or defenses to copyright infringement, including fair use," which should allay many of the concerns referenced above, assuming that the average user has the actual ability to circumvent DRM technology for fair uses, or once the work has entered the public domain.[75] One commentator, however, argues that the DMCA needs to be amended to allow circumvention for all non-infringing uses and not just the current limited exceptions.[76] Moreover, courts have thus far held that § 1201(c) does not allow users to circumvent DRM technology for fair uses. Instead, courts would have fair users exercise their rights only if they can procure a version of the work that has no included DRM technology (if such a copy exists).[77] In other words, a fair user who is not liable under the Copyright Act for infringement of the copyrighted work may still be liable on a separate basis for circumvention of a protection technology.

---

[73] *See* § 1201(a)–(j).

[74] *Id.* § 1201(a)(1)(C)–(D). As discussed in Part III.G, the Librarian of Congress has issued a narrow exemption from the DMCA based on the Sony CD copy protection scandal.

[75] *Id.* § 1201(c).

[76] Blythe, *supra* note 72, at 123–25.

[77] *See Corley*, 273 F.3d at 443 ("Section 1201(c) simply clarifies that the DMCA targets the *circumvention* of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the *use* of those materials after circumvention has occurred. Subsection 1201(c)(1) ensures that the DMCA is not read to prohibit the 'fair use' of information just because that information was obtained in a manner made illegal by the DMCA."); *see also MGM Studios*, 307 F. Supp. 2d at 1102 ("Again, however, while purchasers of DVDs with material in the public domain unquestionably have the right to make use of this public domain material, they can simply access it from a non-CSS encrypted DVD or can choose to access and copy this public domain material in a non-digital form."); United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1141 (N.D. Cal. 2002) ("[T]he argument that Congress' ban on the sale of circumvention tools has the effect of allowing publishers to claim copyright-like protection in public domain works is tenuous and unpersuasive.").

Violation of the DMCA's anti-circumvention provisions subjects the violator to civil and criminal liability.[78] A violator's civil liability can include injunctive prohibitions, impoundment of devices or products involved in a violation, actual or statutory damages, and court costs.[79] A violator's criminal liability can include a fine not to exceed $500,000 and imprisonment not to exceed five years for the first offense; however, criminal liability requires that the circumvention be willful "and for purposes of commercial advantage or private financial gain," which should theoretically exclude some fair users from criminal liability.[80] Facing potential civil or criminal liability, a consumer who encounters especially intrusive DRM technology (such as that included on Sony's CDs in 2005), is posed with a difficult choice: do nothing, and be subject to software that hides files, drains resources, and creates security holes; or risk liability under the DMCA by attempting to remove the software or prevent it from installing on their system.[81]

The congressional purpose behind the DMCA, and the courts' subsequent enforcement, indicate that the legislative and judicial branches of government have embraced the DMCA's protection of DRM technology as a legitimate form of self-help for copyright owners.[82] Such a result is certainly plausible since DRM technology is

---

[78] *See* 17 U.S.C. §§ 1203–1204 (2000).

[79] *Id.* § 1203. Of course, if the violator had breached the prohibition against circumvention for a fair use, the copyright owner would be able to show only nominal *actual* damages; in the case of a fair use, however, assuming that a copyright owner would want the negative publicity that would be associated with bringing suit for a fair use violation of the DMCA, *statutory* damages between $200 and $2,500 per violation would still be available against the violator. *Id.* § 1203(c). While this cost may not be excessive, it would still be a hefty price to pay for a use that is available to consumers as a matter of right under the Copyright Act. *See id.*

[80] *Id.* § 1204.

[81] *See id.* If the software itself collects and disseminates personal information, a consumer could probably circumvent that software so long as the circumvention was limited to the part of the DRM technology that performed that function. *Id.* § 1201(i). Sony's software apparently did collect and disseminate personal information (and created security holes that made this type of activity possible), so this exception could apply to the Sony software. Bruce Schneier, *Real Story of the Rogue Rootkit*, Nov. 17, 2005, WIRED, http://www.wired.com/news/privacy/0,1848,69601,00.html ("Sony claimed the rootkit didn't phone home when it did.").

[82] *See, e.g.*, §§ 1201–05; *Corley*, 273 F.3d at 443; *MGM Studios*, 307 F. Supp. 2d at 1102; *Elcom*, 203 F. Supp. 2d at 1141.

usually so integrated with the work it protects that it could be interpreted to be an inherent characteristic of the product. Under this theory, consumers would be compelled to accept the product's limitations when they purchase the product. However, even under such pretenses, copyright owners need to provide consumers with adequate notice which fully discloses what types of uses the DRM technology restricts, because without such notice, consumers cannot freely accept product limitations imposed by DRM.[83] In the meantime, presumptive judicial and legislative acceptance of DRM incorporation in copyrighted works leaves consumers seeking protection from potentially overreaching DRM schemes outside of the Copyright Act and DMCA (barring revision of those statutes).

III. THE SONY CD COPY PROTECTION SCANDAL OF 2005

A. SONY'S SOFTWARE AND THE ACCOMPANYING END-USER LICENSE AGREEMENT

The software that Sony utilized to protect its CDs from copyright infringement—United Kingdom-based First4Internet's Extended Copy Protection ("XCP") and SunComm's MediaMax—acted as both DRM technology and spyware.[84] As DRM technology, the software allowed consumers to make a limited number of copies (usually three) of protected CDs. However, the software copied the Sony CDs in such a way that consumers could not use those copies to produce additional copies.[85] This type of reproduction, known as "sterile burning," enforced DRM restrictions more effectively when combined with the limitation on the number of copies that consumers could make with the original CD.[86]

When users inserted a protected CD into their computer's CD or DVD drive, an EULA appeared on their monitors stating that software on the CD would "'install a small proprietary software program' that

---

[83] Christopher D. Kruger, Comment, *Passing the Global Test: DMCA § 1201 as an International Model for Transitioning Copyright Law into the Digital Age*, 28 HOUS. J. INT'L L. 281, 286 (2006).

[84] Mark's Blog, *supra* note 3.

[85] *Sony Tests Technology to Limit CD Burning*, CNET NEWS.COM, June 1, 2005, http://news.cnet.co.uk/digitalmusic/0,39029666,39189658,00.htm.

[86] *Id.*

[would] remain there 'until removed or deleted'".[87] If users did not agree to the EULA, they could not access the tracks on their CDs.[88] Prior to acceptance of the EULA, the DRM software monitored other programs running on the user's computer, and if any of the programs could be found on a list of about 200 CD ripping and copying applications, a warning appeared on the user's screen indicating that the user had to close the ripping or copying program before the user could access the CD.[89] The software ejected the CD and closed the application if the user did not comply within thirty seconds.[90]

Once installed, the software examined each disc inserted into the user's computer and determined whether it was protected or not. If it was a protected disc, the software monitored for programs reading the audio tracks and corrupted the audio before it could reach the reading program.[91] The only way that the software allowed a user to copy or listen to protected CDs was through a proprietary media player provided with the CD, and any copies created had DRM restrictions embedded to prevent any further copying.[92]

The XCP and MediaMax DRM software acted like spyware in many ways.[93] Both transmitted information about user listening habits to vendors.[94] The data collected included the user's IP address, and the date, time, and name of the album in the user's computer.[95] Additionally, the MediaMax software installed and ran prior to displaying the EULA, and even if the user did not agree, the software remained installed on the user's computer.[96] Along with the DRM software, the installer for the XCP software also installed a program

---

[87] Krebs, *supra* note 5.

[88] *Id.*

[89] J. ALEX HALDERMAN & EDWARD W. FELTEN, LESSONS FROM THE SONY CD DRM EPISODE 6 (2006).

[90] *Id.*

[91] *Id.* at 9.

[92] *Id.* at 13.

[93] *Id.* at 14.

[94] *Id.*

[95] *Id.*

[96] *Id.* at 7.

that effectively concealed any files associated with the DRM software from the user (similar to a rootkit).[97] This rootkit-like software also caused system instability, drained system resources, and created operating system security holes that hackers could potentially exploit.[98] Finally, the XCP and MediaMax software was difficult to remove because neither included any uninstallation software and the XCP software hid files, making it virtually impossible for the average user to delete or uninstall the software.[99] Moreover, when Mark Russinovich found the XCP files and deleted them, his CD drive crashed.[100]

Even though it described what users could generally do with music on protected CDs, the EULA that accompanied the XCP and MediaMax software generally failed to fully disclose the nature of the software that would be installed onto their computers.[101] Ineffective or nonexistent notice is one of the defining characteristics of spyware applications. Sony's MediaMax EULA informed users that the software did not collect personal information, despite the apparently contrary collection of personal information.[102] The EULAs conditioned use of digital files on users' continued ownership of the corresponding CD,[103] and Sony reserved the right to use all software, and the accompanying media player, to enforce protection of its intellectual property assets without providing prior notice of such

---

[97] *Id.* at 18–19.

[98] *Id.* at 19–20; Mark's Blog, *supra* note 3; Krebs, *supra* note 5. "Sony's software could help hackers circumvent most antivirus products on the market today . . . installing the Sony program on a machine running Windows Vista—the beta version of the next iteration of Microsoft Windows—'breaks the operating system spectacularly.'" Krebs, *supra* note 5.

[99] HALDERMAN & FELTEN, *supra* note 89, at 20.

[100] Mark's Blog, *supra* note 3.

[101] BMG Digital Content EULA, http://www.cs.princeton.edu/~jhalderm/cd3/bmg-eula.html (last visited Feb. 27, 2008); Steven Vaughan-Nichols, *Sonys Rootkit DRM Raises Legal Red Flags*, EWEEK, Dec. 1, 2005, http://www.eweek.com/c/a/Linux-and-Open-Source/Sonys-Rootkit-DRM-Raises-Legal-Red-Flags/.

[102] BMG Digital Content EULA, *supra* note 101; discussion *supra* Part III.A.

[103] BMG Digital Content EULA, *supra* note 102; Vaughan-Nichols, *supra* note 101. For example, if users gave the CD away, or even if they lost the CD or a thief stole it from them, the EULA terminated users' rights to any copies that were still in their possession. Vaughan-Nichols, *supra* note 101.

enforcement.[104] Both EULAs generally disclaimed any warranties that consumers might assert and placed risks of loss or damage on the consumer.[105] Both EULAs also purported to limit the liability of Sony and corresponding parties under a wide array of legal theories arising out of the EULA terms or the use of the protected materials.[106] Sony reserved the right to update the software as it saw fit; if users did not update the software, their license to use the protected materials could be terminated.[107] Finally, the EULAs contained forum clauses mandating that disputes be resolved in the state of New York, outside the presence of a jury.[108]

B. SONY'S INITIAL STEPS AND MOTIVATIONS

Following testing of its DRM software, Sony began releasing CDs containing the software in March of 2005.[109] By the time Mark Russinovich discovered the rootkit software, Sony had shipped over 4.7 million CDs containing the software, and consumers had already purchased 2.1 million of those CDs.[110] Initial estimates speculated that the software had been installed onto over half a million computers.[111] Thomas Hesse, President of Global Digital Business at Sony BMG, noted that fighting casual ripping and burning of CDs was a major concern for his company because two-thirds of all piracy arises from those activities.[112] During the last decade, dealing with CD piracy had become a serious issue for the recording industry. Early on, the recording industry focused mainly on Internet file swapping, but by 2005, the recording industry shifted its focus to widespread CD

---

[104] BMG Digital Content EULA, *supra* note 101; Vaughan-Nichols, *supra* note 101.

[105] BMG Digital Content EULA, *supra* note 101; Vaughan-Nichols, *supra* note 101.

[106] BMG Digital Content EULA, *supra* note 101; Vaughan-Nichols, *supra* note 101.

[107] Vaughan-Nichols, *supra* note 101.

[108] BMG Digital Content EULA, *supra* note 101; Vaughan-Nichols, *supra* note 101.

[109] *Sony Tests Technology to Limit CD Burning*, *supra* note 85.

[110] Borland, *supra* note 4.

[111] Schneier, *supra* note 81.

[112] *Sony Tests Technology to Limit CD Burning*, *supra* note 85.

burning.[113] Recent research had shown that consumers obtained twenty-nine percent of their new music through ripping or burning music CDs.[114] Record companies, including Sony BMG, felt that piracy had caused the industry to lose $4.2 billion each year and, to Sony, DRM technology potentially provided an answer to declining sales.[115]

C. THE PUBLIC REACTION

The result of Russinovich's October 31, 2005 discovery of Sony's spyware-like DRM software was public outrage.[116] Music fans called for a boycott against Sony.[117] Journalists argued that Sony's behavior constituted security malpractice.[118] Upon discovering that the DRM software was on Department of Defense computers, the Department of Homeland Security publicly reprimanded Sony by saying, "It's your intellectual property. It's not your computer."[119] Amazon.com offered refunds to customers who bought Sony DRM CDs from the website.[120] Microsoft announced that it would provide security updates to Windows users to remove the DRM software.[121] On November 10, 2005, the first virus exploiting the Sony DRM software appeared, only ten days after Russinovich's discovery.[122]

---

[113] Borland, *supra* note 1.

[114] *Id.*

[115] Krebs, *supra* note 5.

[116] *Id.*

[117] *Id.*

[118] eWEEK Editorial Board, *Rootkit DRM Constitutes Security Malpractice*, Nov. 28, 2005, EWEEK, http://www.eweek.com/article2/0,1895,1893785,00.asp.

[119] Dave Methvin, *The Sony XCP Rootkit*, PCPITSTOP, Nov. 25, 2005, http://www.pcpitstop.com/spycheck/sonyxcp.asp.

[120] *Id.*

[121] Joris Evers, *Microsoft Will Wipe Sony's 'Rootkit'*, CNET NEWS.COM, Nov. 13, 2005, http://news.com/Microsoft-will-wipe-Sonys-rootkit/2100-1002_3-5949041.html.

[122] John Borland, *Bots for Sony DRM Rootkit Spotted Online*, CNET NEWS.COM, Nov. 11, 2005, http://news.cnet.co.uk/digitalmusic/0,39029666,39194060,00.htm.

Adding insult to injury, Sony and the DRM software developers' initial reaction was nonchalant.[123] The CEO of First4Internet stated, "I think this is slightly old news . . . . For the eight months that these CDs have been out, we haven't had any comments about malware (malicious software) at all."[124] Sony BMG's president of global digital business stated that "Most people don't even know what a rootkit is, so why should they care about it?"[125] Researchers found that Sony's uninstallation patch contained serious security holes.[126] Sony first announced that it would stop shipping CDs with the software (but would not say which CDs had the software on them), then finally announced a recall of CDs remaining on store shelves, offered to exchange DRM-less CDs with consumers who had bought the CDs with DRM on them, and provided a list of CDs containing the controversial software.[127]

D. INVESTIGATIONS

In response to the discovery of Sony's rootkit software, Florida and New York began civil investigations of Sony, and the Milan, Italy-based Association for Freedom in Electronic Interactive Communications-Electronic Frontiers Italy ("ALCEI-EFI") urged Italian prosecutors to initiate a criminal investigation of Sony.[128] The New York Attorney General's office found in its investigation that CDs containing Sony's software could still be purchased from retail stores more than a week after Sony had recalled the CDs.[129] In a written

---

[123] Borland, *supra* note 1.

[124] *Id.*

[125] Schneier, *supra* note 81.

[126] Methvin, *supra* note 119.

[127] *Id.* This source contains a hyperlink to the complete list of CDs containing Sony's DRM software.

[128] Arik Hesseldahl, *Spitzer Gets on Sony BMG's Case: New York's Attorney General has Turned His Attention to Sony BMG's Copyright-Protection Fiasco*, BUSINESSWEEK, Nov. 29, 2005, http://www.businessweek.com/technology/content/nov2005/tc20051128_573560.htm; Posting of Kurt Opsahl to Electronic Frontier Foundation Deeplinks Blog, http://www.eff.org/deeplinks/archives/004292.php (Jan. 3, 2006); Robert McMillan, *Italian Police Asked to Investigate Sony DRM Code: Also, Computer Associates Brands Sony Code 'spyware'*, PC WORLD, Nov. 7, 2005, http://www.pcworld.com/article/id,123454-page,1/article.html.

[129] *Id.*

statement, New York Attorney General Elliot Spitzer stated that "[i]t is unacceptable that more than three weeks after this serious vulnerability was revealed, these same CDs are still on shelves, during the busiest shopping days of the year [late November of 2005]."[130] As investigations of Sony's DRM software continued, thirty-six other states and the District of Columbia joined Florida and New York in a consortium led by Massachusetts.[131] The states alleged that Sony's software created security holes which lead to potential computer failure, that Sony failed to inform consumers of the nature or existence of the software, and that the XCP software specifically hid itself from consumers once downloaded to their computers.[132] According to Ohio Attorney General Jim Petro:

> "The Consumer Sales Practices Act states that all terms of a product must be disclosed to the consumer before they buy it. Sony's hidden software violated Ohio laws and put consumers' computers at risk . . . . Companies selling CDs and computer software need to disclose all that the consumer will be getting with the purchase."[133]

This investigation never became a formal lawsuit; Massachusetts announced on December 21, 2006, that it had reached a settlement agreement in which Sony agreed to pay $4.25 million to the consortium and up to $175 to consumers whose computers were damaged by Sony's software.[134] Additionally, "[t]he injunctive relief

---

[130] *Id.*

[131] Greg Sandoval, *Sony BMG Settles Rootkit Case with 39 States*, CNET News.com, Dec. 21, 2006, http://news.com.com/Sony+BMG+settles+rootkit+case+with+39+states/2100-1027_3-6145714.html. The members in the consortium included Alabama, Alaska, Arizona, Arkansas, Connecticut, Delaware, Florida, Idaho, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming, and the District of Columbia. *See Ohio, 39 States Settle with Sony BMG over Anti-copying Software*, INS. J., Dec. 28, 2006, http://www.insurancejournal.com/news/midwest/2006/12/28/75485.htm.

[132] *Ohio, 39 States Settle with Sony BMG over Anti-copying Software*, *supra* note 131.

[133] *Id.*

[134] Press Release, Massachusetts Attorney General Tom Reilly, AG Reilly Secures $4.25 Million Settlement with Sony BMG: Leads 40 States to Resolve Hidden Anti-copying Software Issue (Dec. 21, 2006); Sandoval, *supra* note 131 ("The 13 states that started the

provisions of the settlement will specifically prohibit SONY BMG from using XCP or MediaMax DRM software in the future, and will sharply limit the ways in which anti-copying software may be used in the future."[135] As of this writing, no information appears to be available regarding the result of the Commander-in-Chief of the Fraud Contrast Group of the Financial Police in Italy's ("Guarda di Finanza") criminal investigation prompted by ALCEI-EFI or whether such an investigation has even taken place. ALCEI-EFI asked the Guarda di Finanza to "identify the authors of the software, and those who made the willful decision of distributing it in a hidden form, and also detect if other organizations committed similar abuses."[136] According to ALCEI-EFI, guilty persons could be charged with "arbitrarily 'self-made' justice, intentional damage to computer systems, and diffusion of software that damages information and communication systems."[137] The Federal Trade Commission initiated its own investigation into Sony's software. The FTC and Sony settled this investigation on terms similar to those in the state consortium settlement agreement, including compensation for damage to computers, exchange of CDs, limitations on Sony's use of DRM software in the future, and monitoring by the FTC to ensure compliance with the agreement.[138]

E. CLASS ACTIONS FILED AGAINST SONY

Individuals filed several lawsuits against Sony in November 2005.[139] These included *Guevara v. Sony BMG Music*

---

settlement process with Sony BMG will each receive $316,538, while the rest will get $5,000.").

[135] *Ohio, 39 States Settle with Sony BMG over Anti-copying Software*, *supra* note 131.

[136] Press Release, ALCEI, Legal Proceedings in Italy by ALCEI Against Sony for a "Criminal" Offense: In a Frenzy of Attempts to Prevent Music Reproduction, Sony BMG Entertainment Distributes Dangerous Software (Nov. 4, 2005), *available at* http://www.alcei.org/?p=22.

[137] *Id.*

[138] *Sony BMG Settles FTC "Rootkit" Charges*, CONSUMERAFFAIRS.COM, Jan. 31, 2001, http://www.consumeraffairs.com/news04/2007/01/ftc_sony_bmg.html.

[139] Ingrid Marson, *Sony Settles 'Rootkit' Class Action Lawsuit*, CNET NEWS.COM, Dec. 29, 2005, http://news.com.com/Sony+settles+rootkit+class+action+lawsuit/2100-1002_3-6012173.html.

Entertainment,[140] *Michaelson v. Sony BMG Music, Inc.*,[141] *Hull v. Sony BMG Music Entertainment* ("The EFF Suit"),[142] and *Bahnmaier v. Sony BMG Music Entertainment*,[143] among others.[144] On December 29, 2005, lawyers in *Michaelson* reached a settlement agreement benefiting all affected persons in the United States.[145] In the settlement agreement, Sony agreed to immediately recall all of its CDs containing the XCP software (but not the MediaMax software) and replace them with unprotected CDs.[146]

Sony agreed to compensate consumers by allowing them to: either (1) download three albums over the Internet or (2) download one album and accept a $7.50 reimbursement.[147] Sony also agreed to (1)

---

[140] Guevara v. Sony BMG Music Entm't, No. BC342359 (Cal. Super. Ct. Nov. 1, 2005). This case sought relief for a class limited to California citizens and alleged violations of section 1770(a) of the California Civil Code (misrepresentation), sections 22947.3 (taking control of computer resources), and 17200 (unfair, unlawful, and fraudulent business practices) of the California Business and Professions Code. Complaint at 8–10, *Guevara*, No. BC342359, *available at* http://www.sonysuit.com/classactions/guevara/complaint.pdf.

[141] Michaelson v. Sony BMG Music, Inc., No. 05 CV 9575 (NRB) (S.D.N.Y. Nov. 14, 2005). This case was eventually consolidated with others as a national (federal) class action and alleged violations of federal computer fraud law, common law trespass, and common law fraud. Complaint at 12–14, *Michaelson*, No. 05 CV 9575 (NRB), *available at* http://www.sonysuit.com/michaelson/complaint.pdf.

[142] Hull v. Sony BMG Music Entm't, No. BC343385 (Cal. Super. Ct. Nov. 21, 2005). This case, filed by the Electronic Frontier Foundation, was another class action for Californians and alleged similar violations to the *Guevara* case, and added claims for breach of implied covenant of good faith and fair dealing under California contract law and false or misleading statements in violation of section 17500 of the California Business and Professions Code. Complaint at 23–28, *Hull*, No. BC343385, *available at* http://www.sonysuit.com/classactions/eff/complaint.pdf.

[143] Bahnmaier v. Sony BMG Music Entm't, No. CJ 2005 06968 (Okla. Dist. Ct. Nov. 28, 2005). This case was a class action for Oklahoma residents and included claims for negligence, trespass to chattels, fraud, invasion of privacy, breach of implied warranty of merchantability, and violation of the Oklahoma Consumer Protection Act. Complaint at 12–15, *Bahnmaier*, No. CJ 2005 06968, *available at* http://www.sonysuit.com/classactions/bahnmaier/complaint.pdf.

[144] *See* Mark Lyon, *Class Action Lawsuits*, SONYSUIT.COM, Nov. 30, 2005, http://www.sonysuit.com/classactions/.

[145] Marson, *supra* note 139.

[146] *Id.*

[147] *Id.*

cease production of CDs with the harmful DRM software; (2) provide technical support to correct any vulnerabilities (presently known or later discovered) caused by the software; (3) not collect any personally identifiable information about consumers through the software; (4) destroy any other information collected by the software after ten days; (5) initiate an independent investigation regarding its collection of personal information; (6) waive several provisions of the XCP and MediaMax EULAs; (7) ensure that future DRM software (until 2008) installs on consumer computers pursuant to active consent by the consumer; (8) provide uninstallation software for DRM software (until 2008); (9) provide clear and accurate EULAs for DRM software and submit those EULAs to independent review (until 2008); (10) submit future DRM software to an independent reviewer and obtain an opinion that the software is safe for consumers (until 2008); and (11) provide notice that a CD contains DRM software on the CD's packaging materials.[148]

Canadian plaintiffs filed similar class actions against Sony in their country.[149] The settlement agreement in those cases initially mirrored the United States version, with the exclusion of the provisions in the United States regulating Sony's future use of DRM software (e.g., independent review requirements for DRM software and the accompanying EULA).[150] The Canadian Internet Policy and Public Interest Clinic ("CIPPIC") quickly objected, and the Canadian court hearing the case required Sony to provide notice to Canadian class counsel and CIPPIC if it uses any DRM software in the future that has not been independently evaluated and verified as safe for consumer use.[151] In addition, the CIPPIC filed complaints with five government agencies, effectively voiding Sony's main rationale for not including

---

[148] Settlement Agreement at 20–29, *In re* Sony BMG CD Techs. Litig., No. 1:05-CV-09575 (NRB) (S.D.N.Y. Dec. 28, 2005), *available at* http://www.sonysuit.com/classactions/michaelson/settle.pdf.

[149] Michael Geist, Sony Hit with Canadian Class Action Suits, Jan. 5, 2006, http://www.michaelgeist.ca/index.php?option=com_content&task=view&id=1062&Itemid=89&nsub.

[150] *Canadian Sony Rootkit Settlement Misses the Mark*, EFFECTOR, Sept. 13, 2006, http://w2.eff.org/effector/19/35.php (scroll midway down the page to see the article).

[151] *Calling Sony BMG's Bluff: Canadian Rootkit Settlement Improved*, EFFECTOR, Sept. 25, 2006, http://w2.eff.org/effector/19/37.php (scroll to the bottom third of the page to see the article).

the injunctive provisions from the U.S. settlement agreement in the Canadian settlement agreement.[152]

F. THE TEXAS AND CALIFORNIA CONSUMER PROTECTION LAWSUITS

Texas Attorney General Greg Abbott filed a lawsuit against Sony on behalf of the state of Texas on November 21, 2005.[153] The lawsuit claimed that Sony's DRM software had violated the Texas Spyware Act; specifically, the XCP software's rootkit attributes—hiding files, installing without user consent, monitoring user activities, and difficulty of removal—raised Abbott's suspicions and prompted the Texas suit.[154] One month later, Abbott amended the claims of the lawsuit to include allegations that Sony's failure to adequately disclose the nature of its software to consumers violated the Texas Deceptive Trade Practices Act.[155]

Sony settled the Texas lawsuit and a similar California lawsuit on December 19, 2006.[156] In the settlement, Sony agreed to pay each state $750,000 in damages and expenses and refund up to $175 to each consumer harmed by Sony's DRM software.[157] Sony also agreed to "destroy any existing CDs embedded with the problematic DRM technology, continue working to withdraw those CDs from the marketplace, and submit to independent, third-party monitoring of any software-enhanced music CDs for the next five years."[158]

---

[152] *Id.* Sony had previously argued that it agreed to provisions regulating future DRM software use in the United States under mounting pressure from state investigations; before CIPPIC filed complaints in Canada, Sony had not felt any governmental pressure in that country. *Id.*

[153] Abbott Press Release, *supra* note 7.

[154] *Id.*

[155] Press Release, Texas Attorney General Greg Abbott, Attorney General Abbott Slaps Sony With New Spyware Violations (Dec. 21, 2005), *available at* http://www.oag.state.tx.us/oagnews/release.php?id=1370.

[156] Jennifer LeClaire, *Sony Antes Up $1.5 Million to Settle DRM Suits*, TECHNEWSWORLD, Dec. 21, 2006, http://www.technewsworld.com/story/54840.html.

[157] *Id.*

[158] *Id.*

G. THE LIBRARIAN OF CONGRESS'S EXEMPTION BASED ON THE SONY CD COPY PROTECTION SCANDAL

On November 27, 2006, pursuant to the DMCA, the Librarian of Congress issued a narrow exemption based largely on the facts of the Sony CD copy protection scandal.[159] Essentially, for the three-year period following that date, the DMCA's prohibition against circumvention of technological measures that effectively control access to copyrighted works will not apply to people making a noninfringing use of a copyrighted work that falls into the following class:

> Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.[160]

The Register of Copyrights noted that this exemption was directly related to the facts of the Sony CD copy protection scandal.[161] The Register also noted that, while it was possible that the type of activity exempted may have already been allowed under 17 U.S.C. § 1201(j), the applicability of § 1201(j) was unclear.[162] Recognizing the seriousness of the problem posed by the Sony CD copy protection scandal and the need for researchers to engage in the excluded activities, the Register recommended this limited exclusion, which the Librarian of Congress subsequently adopted.[163] While the exemption is a step towards providing consumer protection from DRM misuse, it is far too narrow.

---

[159] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68, 472–80 (Nov. 27, 2006) (codified at 37 C.F.R. pt. 201).

[160] *Id.* at 473–74.

[161] *Id.* at 472–80.

[162] *Id.* at 477.

[163] *Id.* at 479.

H. SONY STRIKES BACK

On July 3, 2007, Sony BMG filed a lawsuit against SunComm (now known as the Amergence Group, Inc.), producer of the MediaMax DRM software, in the Supreme Court of New York for New York County.[164] The lawsuit sought $12 million in damages from SunComm for breach of contract, false advertising, unfair and deceptive acts and practices, negligence, and indemnification under the software license agreement between the two companies.[165] It appears that Sony BMG has voluntarily discontinued the suit.[166] If it had reached trial, the lawsuit likely would have explored interesting evidence regarding the respective amounts of knowledge that Sony BMG and SunComm had regarding the effect that the MediaMax DRM software would have on consumers and the amount of testing that Sony and SunComm subjected the software to before making the decision to introduce it to the marketplace. Moreover, the lawsuit would have considered several unsettled legal issues, including (1) various factors contributing to fault or providing defenses to liability for these types of claims; (2) the level of care required of a software developer that develops defective DRM software with the knowledge that it will reach consumers; (3) the level of care required of a copyright owner that makes the decision to make defective DRM software available for public consumption; and (4) the appropriate apportionment of fault between such DRM software developers and copyright owners.

IV. MANAGING DIGITAL RIGHTS MANAGEMENT: SUGGESTED SOLUTIONS

The Sony CD copy protection scandal provides an example of an attempt by a copyright owner to use DRM technology that went astray. Although some copyright holders are beginning to experiment

---

[164] *Sony BMG Sues CD Software Firm*, HOLLYWOOD REP., July 12, 2007, http://www.hollywoodreporter.com/hr/content_display/business/news/e3i214c26acb62c59b679bbbc3594def806.

[165] Summons at 1–2, Sony BMG Music Entm't v. Amergence Group Inc., No. 07602201 (N.Y. Sup. Ct. July 3, 2007), *available at* http://iapps.courts.state.ny.us/iscroll/C_PDF?CatID=250946&CID=602201-2007&FName=0.

[166] County Clerk Minutes, Sony BMG Music Entm't v. Amergence Group Inc., No. 07602201 (N.Y. Sup. Ct. July 3, 2007), *available at* http://iapps.courts.state.ny.us/iscroll/CCMinutes.jsp?IndexNo=602201-2007.

with distributing their content without DRM technology,[167] DRM will most likely continue to be used in a wide variety of contexts for the foreseeable future. As evidenced by the Sony products, the potential remains to misuse DRM, and it is imperative to determine whether currently existing law is sufficient to prevent or deter such DRM misuse in the future.

A. THE NEED FOR INDEPENDENT DIGITAL RIGHTS MANAGEMENT REGULATION

Proponents of the view that DRM does not need to be regulated argue that the federal government should remain neutral on DRM.[168] To achieve this neutrality, these proponents would require that Congress amend the DMCA to prohibit circumvention for the purpose of copyright infringement only.[169] Advocates of government neutrality state that requiring the government to oversee and regulate DRM would be too costly and expensive.[170] Conversely, neutrality advocates believe that DRM regulation is unnecessary because the market reaction to DRM schemes will cause intellectual property owners to change their DRM policies accordingly, or perhaps do away with DRM altogether.[171]

However, overly intrusive DRM schemes continue to violate consumers' rights. The Sony CD copy protection scandal, described in this comment, provides one example of DRM software that violates both of these rights.[172] In another example of intellectual property owners' apparent willingness to violate consumer rights, Twentieth Century Fox shipped the German version of its *Mr. & Mrs. Smith* DVD with a DRM scheme having rootkit-like attributes similar to Sony's.[173]

---

[167] Candace Lombardi, *iTunes Goes DRM-Free with EMI*, CNET NEWS.COM, May 30, 2007, http://www.news.com/iTunes-goes-DRM-free-with-EMI/2100-1027_3-6187457.html.

[168] McCullagh & Homsi, supra note 24, at 327.

[169] *Id.*

[170] *Id.* at 324–25.

[171] *Id.* at 326–27 (describing various consumer reactions and the corresponding effect on intellectual property owners' DRM policies).

[172] *Id.*

[173] Ryan Naraine, *Mr. & Mrs. Smith DVD Ships with Rootkit-like DRM*, eWEEK, Feb. 14, 2006, http://www.eweek.com/article2/0,1795,1926917,00.asp.

Symantec also recently shipped its Norton Systemworks software with rootkit-like functionality.[174] In light of continuing use of DRM schemes to violate the rights of others, a proposal for a new regulatory scheme may prove useful.

1. PROBLEMS WITH EXISTING REMEDIES

Federal statutory remedies for future cases similar to the Sony CD copy protection scandal include the Computer Fraud and Abuse Act, the Federal Trade Commission Act, and the Electronic Communications Privacy Act.[175] For example, the Computer Fraud and Abuse Act could address almost all activity that meets common definitions of spyware so long as the activity results in aggregate loss of over $1,000 in a one-year period.[176] Alternatively, the Electronic Communications Privacy Act could provide a remedy for interception or access of electronic communications by overreaching DRM software.[177] Finally, the FTC has utilized the Federal Trade Commission Act to bring claims of deceptive trade practices against spyware producers, and could likely do the same to copyright owners who utilize overreaching and deceptive DRM.[178]

State and common law remedies include state deceptive trade practices acts, anti-spyware legislation, unfair competition statutes, and common law concepts such as trespass to chattels and conversion.[179] To the extent that DRM technology in the future fails to disclose material aspects of its operation, acts deceptively, causes damage to consumer electronics devices and computers, or "spies" on consumers, such state law theories may well provide a basis for recovery.[180]

---

[174] Ryan Naraine, *Symantec Caught in Norton 'Rootkit' Flap*, eWEEK, Jan. 11, 2006, http://www.eweek.com/article2/0,1795,1910077,00.asp.

[175] Crawford, *supra* note 16, at 1464–68.

[176] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000).

[177] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2712 (1986).

[178] *See* Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2004) (declaring unlawful "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.").

[179] Crawford, *supra* note 16, at 1466–68.

[180] *Id.*

There are several problems, however, with relying on current law as the sole means of controlling DRM misuse. To the extent that state laws attempt to regulate copyrighted material and protection technologies protected by the DMCA, such state laws may be preempted by the Copyright Act, which "is expressly intended to create a federal law of uniform, nationwide application by broadly preempting state statutory and common-law copyright regulation."[181] Furthermore, any attempt to regulate DRM as spyware—to the extent that such regulations involve transmissions of information over the Internet—will affect at least some interstate commercial activity and may be subject to challenge under the Dormant Commerce Clause.[182] Anti-spyware and other state legislation applied to DRM technology will also result in inconsistent regulations between the states, increasing the difficulty of compliance and the likelihood that such legislation will make courts "uncomfortable."[183]

In addition to these issues with the application of state law to DRM misuse, several practical difficulties exist that may render current law ineffective to prevent or deter DRM misuse. In order for any of the existing laws to be enforced, abusive DRM must first be detected and the source of the abusive DRM must be determined. The ability of software developers to develop undetectable DRM technology, and the almost indistinguishable similarities between DRM and spyware, poses a serious threat to the effectiveness of existing law.

Even if abusive DRM has been detected, in order for existing law to provide redress for the effects of such DRM, potential plaintiffs must have funds to hire an attorney to litigate against the entity responsible for the abusive DRM, or find an attorney willing to take the case on a contingent-fee basis. The relatively low amount of actual damages available, length and cost of litigation, and—in most cases—vastly superior resources of the entity responsible for the abusive DRM will be enough to deter many plaintiffs. With respect to legislation that is enforceable only by a government actor, such as the Federal Trade Commission Act and state anti-spyware legislation, scarcity of government resources imposes a serious obstacle to enforcement against all but the most egregious cases of DRM misuse.

---

[181] Cmty. for Creative Non-Violence v. Reid, 490 U.S. 730, 731 (1989).

[182] Crawford, *supra* note 16, at 1436.

[183] *Id.* at 1444.

Therefore, given the demonstrated challenges and perceived ineffectiveness of existing law, regulation of DRM under the current schemes does not seem advantageous. Furthermore, legislators likely did not contemplate the potential for misuse of DRM technology when they formulated the various laws that now govern. As a result, application of such laws is insufficient to fully meet the unique challenges of DRM regulation.

2. THE LIBRARIAN OF CONGRESS'S EXEMPTION FROM DMCA LIABILITY

As noted above, the Librarian of Congress issued an exemption to the DMCA in response to the Sony CD copy protection scandal. This exemption may provide a disincentive for copyright owners to use DRM technology which meets the definition provided in the exemption by removing the benefit of legal protection from circumvention. The exemption, however, is far too narrow to provide adequate protection for consumers against DRM misuse in the future.

For example, the exemption applies only to "[s]ound recordings, and audiovisual works associated with those sound recordings."[184] Abusive DRM technology that protects any other category of copyrightable work does not fall under the exemption, and there is, therefore, no disincentive for copyright owners to use such DRM technology with those works. In addition, the exemption is limited to works "distributed in compact disc format."[185] Any abusive DRM technology that accompanies, for example, a DVD, digital file, Blu-Ray disc, or is integrated with consumer electronics devices does not fall within the exemption. The exemption is overly specific with respect to the type of abusive behavior that it discourages. For the exemption to apply, the relevant DRM technology must "create or exploit security flaws or vulnerabilities that compromise the security of personal computers."[186] Abusive DRM behaviors other than those described by the exemption, such as the collection of personal information, are not covered. Furthermore, the exemption applies only to abusive DRM that affects personal computers and not other consumer electronic devices that may be equally threatened by the effects of abusive DRM.

---

[184] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68, 472–80 (Nov. 27, 2006) (codified at 37 C.F.R. pt. 201).

[185] *Id.*

[186] *Id.*

Finally, the exemption relieves consumers from liability for circumventing DRM technology that compromises their personal computers, but does not, and cannot, provide a parallel exemption for software developers who produce and traffic in technology to be used for that purpose by consumers.[187] "Without some availability of circumvention tools, the DMCA exemptions will, in many cases, extend rights to consumers while the anti-trafficking provisions [of the DMCA] simultaneously deny them the means of exercising those rights."[188] Because the Librarian of Congress's exemption from DMCA liability is so narrow, it does not provide an adequate solution to a broad spectrum of potentially abusive DRM technologies, and is therefore insufficient to protect consumers from the effects of DRM misuse.

B. THE NATURE OF DRM REGULATION

1. GENERAL GUIDELINES

As opposed to the current regulatory patchwork of anti-spyware legislation and cyber-crime statutes, an independent scheme should regulate DRM measures. A regulatory scheme specifically targeting DRM will provide intellectual property owners with notice of exactly what standards their DRM software should meet. Currently, intellectual property owners must guess at whether their DRM software complies with various enacted state laws and pending federal laws. Such a scheme should be implemented at the national level in order to ensure consistency with existing copyright law and uniformity of enforcement.[189]

---

[187] Aaron Perzanowski, *Evolving Standards & the Future of DMCA Anti-circumvention Rulemaking*, 10 J. INTERNET L. 1, 20 (2007).

[188] *Id.* It should be noted that the DMCA does not grant the Librarian of Congress the power to create exceptions to the anti-trafficking provisions. *Compare* 17 U.S.C. § 1201(a)(1)(C) (2000) (commanding the Librarian of Congress to hold rulemaking proceedings to determine whether the anti-circumvention provision has an adverse effect on particular non-infringing use and providing that the anti-circumvention provision will not apply to such uses), *with* 17 U.S.C. § 1201(a)(2) (2000) (prohibiting manufacturing, importing, offering to the public, providing, or otherwise trafficking in technologies for circumvention of technological measures but not providing a parallel ability for the Librarian of Congress to create exceptions to these provisions).

[189] *See Cmty. for Creative Non-Violence*, 490 U.S. at 731 (discussing the uniformity goal of the Copyright Act).

Regulation at the national level will also help DRM regulation to avoid any constitutional challenges based on the Dormant Commerce Clause or preemption. Moreover, the argument that governments should just allow the market to regulate DRM by providing anti-spyware and security software to consumers is inapplicable because the anti-circumvention provisions of the DMCA may make the use of such software to remove or provide protection from DRM illegal.

Critics of the DMCA have argued that it is a mistaken attempt to regulate technology, and that regulation of technology is often ineffective, impossible to enforce, and has unintended consequences that make such regulation more harmful rather than more helpful.[190] These critics hypothesize that the reason that regulation of technology is ineffective, or even harmful, is that regulatory bodies have little understanding of the technology that they regulate. Moreover, technology advances so quickly that any attempt to regulate it will necessarily fail to account for impending advances, and the law will be unable to keep up with such advances as they occur.[191] Despite such arguments against regulation of technology, the reality of the situation is that leaving consumer protection against DRM misuse to non-regulatory forces will only serve to perpetuate the inequitable situation that currently exists. Namely, the DMCA regulates technology by prohibiting many consumer self-help activities, such as the development and distribution of software that negates the effects of DRM misuse, while providing protection to copyright owners who use DRM. Even in the absence of official DRM "regulation," public and private actors will continue to influence and regulate DRM technology through contracts and license agreements, private litigation, public litigation (such as spyware legislation enforcement actions by state attorneys general), and governmental investigations. Taken as a whole, in the limited context of DRM regulation, the overriding concern for the general population of consumers should be for their safety and privacy, and not the advancement of technology. In other words, the advancement of technology may be a legitimate interest that the law should not unduly regulate, but a copyright owner that distributes DRM technology to the public should not be allowed to advocate unbridled advancement of technology in lieu of appropriate testing and design.

---

[190] *See* Stephen J. Bigelow, *Government Attempts to Regulate Technology: Efforts To Control Often Do More Harm Than Good*, PROCESSOR, Nov. 12, 2004, at 11, *available at* http://www.processor.com/editorial/article.asp?article=articles%2Fp2646%2F21p46%2F21p46.asp.

[191] *Id.*

Commentators have argued both for and against allowing federal agencies, such as the Federal Communications Commission ("FCC"), to regulate intellectual property owners' use of DRM technology.[192] Critics argue that allowing governmental actors to implement complex regulations could prove to be extremely costly because governmental actors perform tasks at two to three times the cost of independent actors.[193] Furthermore, many past attempts to reconcile DRM with fair use have resulted in complex systems for determining when and how to allow fair use over DRM technology, such as: (1) "Digital Property Trusts"; (2) third-party decision-makers issuing "keys" for circumventing DRM technology in appropriate circumstances; (3) circumvention technology regulations modeled after firearms regulations; and (4) "modular design" and other mandates designed to ensure that DRM technologies do not bar consumers from access copyrighted works for fair uses or after the copyright term has expired.[194] The most inexpensive, elegant, and effective approach to regulation of DRM technology may be a combination of proposals.[195]

2. CONSISTENCY WITH INTERNATIONAL COPYRIGHT LAW

The DMCA was enacted to give effect to the World Intellectual Property Organization ("WIPO") Copyright Treaty, which states:

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in

---

[192] *Compare* Chad Woodford, Comment, *Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management*, 75 U. COLO. L. REV. 253, 291 (2004) (proposing an FCC-implemented model DRM regulation), *with* McCullagh & Homsi, *supra* note 24, at 324 (criticizing proposals for government-implemented DRM regulations as failing to consider the potentially great cost to the public).

[193] McCullagh & Homsi, *supra* note 24, at 324.

[194] *Id.* at 320–22.

[195] Voluntary self-regulation by the DRM industry could provide an equally effective and less costly alternative to regulation by the federal government. *Cf.* Adam D. Theirer, *Regulating Video Games: Parents or Uncle Sam?*, CATO.ORG, July 14, 2003, http://www.cato.org/pub_display.php?pub_id=3167 (describing the success of the Entertainment Software Ratings Board system for rating computer game content, noting that Senator Joseph Lieberman has called it "'a model' for other industries to follow," and comparing the self-regulatory system favorably to parallel regulatory attempts by the federal government).

> connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.[196]

This broad directive allows for flexibility in implementation so long as it is not so restrictive that it prevents a WIPO member country from providing "adequate" legal protection in compliance with the Treaty.[197] The WIPO Copyright Treaty does not require specific legislation, and as a result, some countries have determined that their existing law provides adequate protection to meet its requirements.[198] Member states are not prevented from choosing to provide a wide array of different legal standards to adequately protect technological measures.[199] For example, the European Union Directive on Copyright encourages member states to permit private copyright owners to establish specific exceptions through practice before enacting exceptions into national law.[200] European Union member states have subsequently adopted such independently tailored pieces of national-level legislation.[201] The most notable deviation in these national European copyright laws is that of France, which was recently amended to impose interoperability requirements on DRM technology used in that country and to establish a regulatory body to enforce the law.[202]

---

[196] World Intellectual Property Organization Copyright Treaty art. 11, Dec. 20, 1996, 11 Stat. 2860, 36 I.L.M. 65 (1996).

[197] *See* World Intellectual Property Organization, Geneva, Switz. Nov. 3–5, 2003, STANDING COMMITTEE ON COPYRIGHT AND RELATED RIGHTS, CURRENT DEVELOPMENTS IN THE FIELD OF DIGITAL RIGHTS MANAGEMENT, *available at* http://www.wipo.int/edocs/mdocs/copyright/en/sccr_10/sccr_10_2_rev.doc.

[198] *Id.*

[199] *See id.*

[200] *Id.* at 72.

[201] *Id.* at 77–79.

[202] Nicolas Jondet, *DRM Watchdog Established in France*, FRENCH-LAW.NET, Apr. 11, 2007, http://French-law.net/index.php?option=com_content&task=view&id=37&Itemid=1. The regulatory body's main concerns are ensuring interoperability of works protected by DRM with various consumer devices and ensuring that DRM measures doe not preclude lawful uses. *Id.* The regulatory body is staffed by independent officials from various areas of the French government, including members of French courts.

Australia's implementation of the WIPO Copyright Treaty is said to be more favorable to consumers than other implementations.[203] For example, the Australian Copyright Amendment ("Digital Agenda") Act 2000 does not specifically prohibit circumvention, but instead focuses on technologies and devices that permit circumvention.[204] Japanese copyright law is similar in that it does not specifically prohibit circumvention.[205]

As demonstrated by its WIPO counterparts, it would seem that the United States could, without straying from its duties under the WIPO Treaty, independently establish a regulatory framework that requires DRM designers to consider consumer interests when developing new technologies. Additionally, France's imposition of interoperability requirements illustrates that government regulation of DRM in the United States might be well received by other countries. Although no set of standards currently exists mandating that DRM technology be designed so as to not violate consumer rights, the United States could exemplify emergent consumer-friendly regulations to other countries. Furthermore, given the size and importance of the U.S. market, and its thriving intellectual property regime, mandating that DRM technology meet certain consumer-safe standards in the United States could have a beneficial impact on DRM technology used in other countries.

C. REGULATION BASED ON SONY SETTLEMENTS

1. GUIDELINES

Professor Michael Geist of the University of Ottawa argues that the settlements from the Sony case should form the blueprint for new DRM regulations.[206] The Sony class action settlements restricted Sony's behavior in several ways that would be applicable to an industry-wide regulatory scheme for DRM technology.[207] Model guidelines based on some of those restrictions could be written as follows:

---

[203] World Intellectual Property Organization, *supra* note 197, at 85.

[204] *Id.* at 85–86.

[205] *Id.* at 91.

[206] Geist, *supra* note 20.

[207] *Id.*

Any protection technology accompanying digital forms of copyrightable works must:

1. Interact with, install on, or otherwise integrate with, a consumer electronic device only after the consumer has provided active consent to the interaction, installation, or other means of integration, provided that such consumer electronic device provides consumers with the ability to consent to such interaction, installation, or other integration;

2. Be capable of complete uninstallation from a consumer electronic device in a manner that is reasonably apparent and easily executed by consumers;

3. Display a clear, accurate, and concise EULA and require the consumer to agree to all material terms prior to the interaction, installation, or other means of integration of the protection technology on a consumer electronic device;

4. Not hide files or other elements associated with the protection technology, change file names, or tamper with consumer electronic device attributes other than as required for installation, uninstallation, and normal, nondeceptive purposes related to the display of the copyrighted material; and

5. Transmit or collect no personally identifiable consumer information.

Owners of copyrighted material seeking to use any protection technology in conjunction with a copyrightable work in digital form must:

A. Submit the EULA describing the terms of use of the copyrighted work and protection technology to a third-party evaluator and obtain an independent opinion that the EULA is clear, accurate, concise, and reasonable;

> B. Submit protection technology to a third-party evaluator and obtain an independent opinion that the technology is safe for consumers;
>
> C. Provide notice to prospective consumers that the copyrightable work is accompanied by protection technology and include a description of how the protection technology will affect the consumer's use of the copyrightable work in comparison to established expectations for that type of work, in that type of medium; and
>
> D. Submit the notice to be provided to prospective consumers to a third-party evaluator and obtain an independent opinion that, prior to purchase by consumers, the notice adequately discloses the fact that protection technology accompanies the copyrightable work and sufficiently describes the effects of such protection technology on consumer use of the copyrightable work in comparison to established expectations for that type of work, in that type of medium.

These guidelines provide a blueprint and fair summary of the relevant terms of the Sony class action settlement agreement. Professor Geist recognizes that a model statute based on the Sony settlement would provide consumers with protection parallel to the protection that the DMCA affords copyright owners though its anti-circumvention provisions.[208]

The cost of third-party evaluation of EULAs and technology found in the above model statute should be borne by intellectual property owners as part of the cost of developing DRM technology since it is the intellectual property owners who enjoy increased efficiency by utilizing DRM technology. Providing for less expensive third-party evaluation, instead of governmental agency intervention, and requiring intellectual property owners to front the evaluation costs, should allay the fears critics who decry the potential expense of proposed regulations.[209] Finally, the proposed regulation is limited in scope to what is required to protect consumers from overly intrusive

---

[208] *Id.*

[209] *See* McCullagh & Homsi, *supra* note 24, at 324.

DRM technology and does not attempt to impose the complex technological design requirements feared by DRM regulation critics.[210]

2. POSSIBLE IMPLEMENTATIONS

One possible means of implementing the above guidelines would be to amend the DMCA to define "technological measure" as any device, software, or other means for controlling use of a work by consumers, as long as such technological measure has also been developed, tested, and certified according to the guidelines.[211] As a result, copyright owners would have to prove that they have developed a technological measure pursuant to the guidelines as a part of showing that a defendant has violated the anti-circumvention or anti-trafficking provisions of the DMCA. In other words, copyright owners would not be able to prove that a defendant had circumvented (or trafficked in circumvention technology) a technological measure without also proving that the technological measure in question meets the amended DMCA's definition. The effect of this implementation would be to protect consumers from abusive DRM by providing a disincentive for copyright owners to utilize technological measures that have not been safely designed, appropriately tested, or that provide inadequate notice to consumers. While this implementation is an indirect method of regulating DRM abuse, it may be enough to encourage the production of consumer-safe DRM.

Such an implementation is attractive because it would not require the establishment or funding of a regulatory body to ensure that new DRM technologies conform to the guidelines. Instead, this implementation would place the determination of whether a specific technological measure has conformed to the guidelines in the hands of a federal judge. Because federal judges receive lifetime appointments, they are more likely to be impartial in determining whether a copyright holder's acts in producing and using its DRM technology have conformed to the guidelines and, consequently, less likely to be susceptible to corporate capture.[212]

---

[210] *See id.*

[211] The DMCA does not currently define "technological measure."

[212] In this context, corporate capture refers to the likelihood that special interests (such as copyright owners) will exert disproportionate influence over a decision maker.

One disadvantage of relying on federal judges to determine whether a technological measure is in compliance with the guidelines is that many federal judges may not have sufficient technical training to determine whether the testing and certification of various aspects of a specific DRM technology have met the legal requirements. Another disadvantage of relying solely on judges to makes this determination is the likelihood that copyright owners seeking to sue under the DMCA will engage in forum shopping in a quest to find a judge more likely to favorably interpret the newly amended DMCA definition.

An alternative scheme to implement the guidelines would be to enact a statute actively requiring that copyright owners wishing to use DRM technology conform with the guidelines prior to making the technology available to consumers. Under such a mode of implementation, the copyright owner would have to conform its behavior to meet the guideline standards prior to using DRM technology. Review of the technology by a regulatory body would then take place pursuant to one of two possibilities. The first possibility would be that the regulatory body would review a copyright holder's compliance with the guidelines upon receiving complaints from consumer through an exercise of its discretion. Enforcement could be achieved by in-depth investigation of suspicious cases, or through random audits of copyright owners. The second possibility would be that the regulatory body would require copyright owners to provide notice of intent to introduce a new DRM technology to consumers, whereupon the regulatory agency would review evidence submitted by the copyright owner to determine whether the technology complies with the guidelines before granting approval for the copyright owner to proceed. Penalties for failure to comply with the regulatory scheme could include loss of copyright, loss of right to sue for circumvention or trafficking, sanctions on the use of the DRM technology, or fines.

One advantage of such a mode of implementation is that it would designate a single body to apply the guidelines, promote uniformity, and increase predictability for copyright owners developing consumer-safe DRM technology. In addition, use of a single regulatory body to oversee compliance will eliminate the forum shopping problem previously discussed; however, care would have to be exercised in selecting members of the regulatory body to minimize the likelihood of corporate capture. Adopting France's approach in determining the composition of the regulatory body may be useful in avoiding the possibility of corporate capture.[213] A significant

---

[213] *See* Jondet, *supra* note 202.

disadvantage of this implementation strategy is that valuable resources must be expended to establish and fund the regulatory body.

D. FAIR USE AND COPYRIGHT TERM EXPIRATION

Critics of DRM and the DMCA have long complained that DRM technologies inhibit consumer access to copyrighted works for fair use after the copyrighted work has entered the public domain. A model statute attempting to address DRM in its entirety should address these issues as well.[214] Many commentators have formulated complex systems for resolving the conflict between the DMCA's anti-circumvention provisions and fair uses allowed by the Copyright Act. A simpler and more elegant solution would be to amend the DMCA to make fair use and other defenses available under the Copyright Act available as defenses to charges of circumvention and trafficking in circumvention technology.[215]

V. CONCLUSION

Congress and the judiciary have implicitly endorsed DRM and similar intellectual property protection measures. While such technological self-help is undoubtedly a valid exercise of rights for intellectual property owners, the Sony CD copy protection scandal illustrates the outer limits of such rights. When intellectual property owners exercise their right to technological self-help in such a way that violates consumer privacy and property rights, they go too far.

While state governments and individual consumers have been able to combat intrusive DRM technology by labeling it as spyware or applying existing legal principles, there are potential problems with anti-spyware legislation and other currently existing remedies. Therefore, it is a dubious means for regulating the overall scope and impact of DRM technology. Furthermore, currently existing legislation and other legal principles are not an appropriate method for addressing DRM because of the unique intersection of consumer rights, intellectual property rights, and cyber-crime that DRM presents. Any attempt to regulate DRM must fully consider the delicate balance between consumer rights and intellectual property holders' interests in protecting copyrightable works.

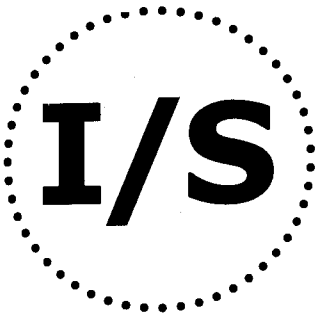
---

[214] Woodford, *supra* note 192, at 291–95 (2004).

[215] *See* McCullagh & Homsi, *supra* note 24, at 327.

To this end, this comment suggests solutions that may provide a blueprint for more complete DRM regulation in the future. While the suggestions in this comment may be incomplete and could be further developed, they describe the general attributes of DRM regulations and the obstacles that such regulations must overcome to allay common criticisms and effectively combat current abuses. These key features include federal implementation of an amended statutory scheme, a simple regulatory regime, and appropriate allocation of the costs to regulate DRM technology. The proposed model regulation provides enhanced consumer protection from potential DRM technology abuses by mandating notice to consumers that a product is protected by DRM technology, requiring clear EULAs, and prohibiting certain deceptive uses of DRM technology. Furthermore, the proposed regulation requires that intellectual property owners wishing to use DRM technology submit the technology and accompanying EULA to third-party evaluators and obtain certification that the technology is safe and that it does not infringe others' intellectual property. Essentially, the accompanying EULA must be clear, concise, and accurate.

This comment suggests that Congress amend the DMCA to restore consumer rights under copyright law, and reverse the limitations of DRM technology that deny consumers legal defenses such as fair use and other recourse under the Copyright Act. Restoration of the appropriate balance between consumer rights and intellectual property owner rights is attainable, and as this Comment demonstrates, there are practical means to avoid the unnecessary costs and complications that are often associated with effecting legislative change.



A Journal of Law and Policy for the Information Society

Sponsored by

The Moritz College of Law
The Ohio State University
Drinko Hall, Room 169
55 West 12th Avenue
Columbus, OH 43210

H. John Heinz III School of
Public Policy and Public
Management
Carnegie Mellon University
Hamburg Hall 1108
5000 Forbes Avenue
Pittsburgh, PA 15213-3890

Please Visit the **I/S** Website to Subscribe Electronically:

is-journal.org

Please subscribe me or my organization to:
I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Name:_____

Organization:_____

Address:_____

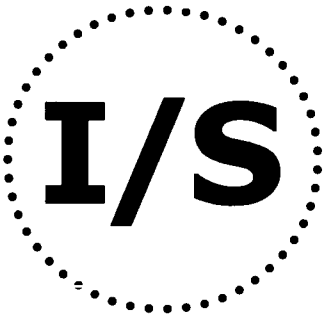
City:_____State:_____Zip Code:_____Country:_____

Telephone:_____Fax:_____Email:_____

Annual Volume Subscription Type (please circle one):

Domestic ($45) – Student w/ID ($20)		Foreign ($100)	
Institutional ($100)		Supporting ($150)	

To make payment now, please enclose check in separate envelope payable to: "**I/S JOURNAL**"



A Journal of Law and Policy for the Information Society

Published by

The Center for Interdisciplinary Law and Policy Studies
The Ohio State University
Drinko Hall
55 West 12th Avenue
Columbus, Ohio 43210

Please Visit the **I/S** Website to Subscribe Electronically:

is-journal.org

Place Stamp Here
Post Office
Will Not Deliver
Mail Without
Postage

BUSINESS REPLY CARD

I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

ATTN: I/S JOURNAL
The Ohio State University
Moritz College of Law
55 West 12th Avenue
Columbus. OH 43210